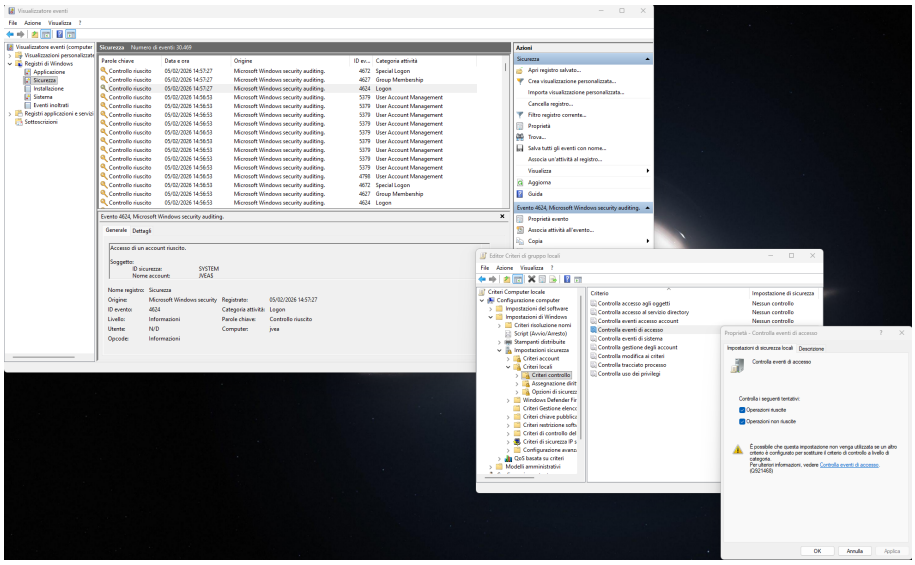
Report Tecnico:
Windows Audit Policy Configuration

Configurazione Criteri di Controllo e Analisi Log

Autore: Josh Van Edward Abanico
Data: 5 febbraio 2026



Obiettivo: Implementazione Logging di Sicurezza & Analisi Eventi
Ambito: System Hardening & Monitoring

Indice

1 Introduzione e Scenario

1.1 Obiettivi

L'obiettivo di questa attività è configurare correttamente le politiche di auditing (controllo) su una workstation Windows per garantire la visibilità sugli eventi di sicurezza critici. Successivamente, si procederà alla verifica della generazione dei log tramite il Visualizzatore Eventi, simulando le attività di raccolta dati tipiche di un SIEM (Security Information and Event Management).

1.2 Ambiente di Test

L'attività è stata svolta su una macchina locale Windows 11.

- **Sistema Operativo:** Microsoft Windows 11
- **Strumento Utilizzato:** Visualizzatore Eventi ('eventvwr').
- **Utente Operatore:** Josh Van Edward Abanico (Account: JVEA)

2 Verifica e Analisi Log (Monitoring)

2.1 Accesso ai Log di Sistema

Una volta applicate le policy, è stato avviato il Visualizzatore Eventi per confermare la generazione dei log.

```
eventvwr
```

Listing 1: Avvio del Visualizzatore Eventi

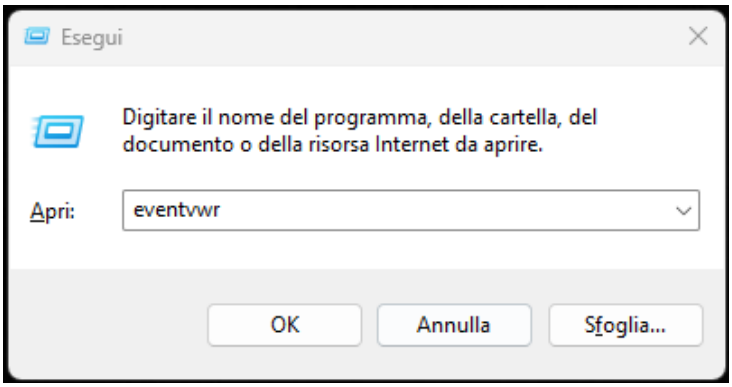


Figura 1: Esecuzione del comando per l'apertura dei log.

2.2 Analisi degli Eventi di Sicurezza

Navigando in **Registri di Windows** → **Sicurezza**, sono stati analizzati gli eventi generati a seguito della nuova configurazione. Sono stati identificati eventi critici che confermano il funzionamento dell'auditing.

2.2.1 Evento ID 4672 - Special Logon

È stato rilevato l'evento con ID **4672**. Questo evento indica che a un nuovo accesso sono stati assegnati privilegi speciali. È un indicatore critico in un SOC poiché spesso associato ad accessi amministrativi o di sistema (es. utente SYSTEM o Administrator).

```
ID Evento: 4672
Categoria: Special Logon
Parole chiave: Controllo riuscito
Soggetto:
    ID Sicurezza: SYSTEM
    Nome Account: SYSTEM
```

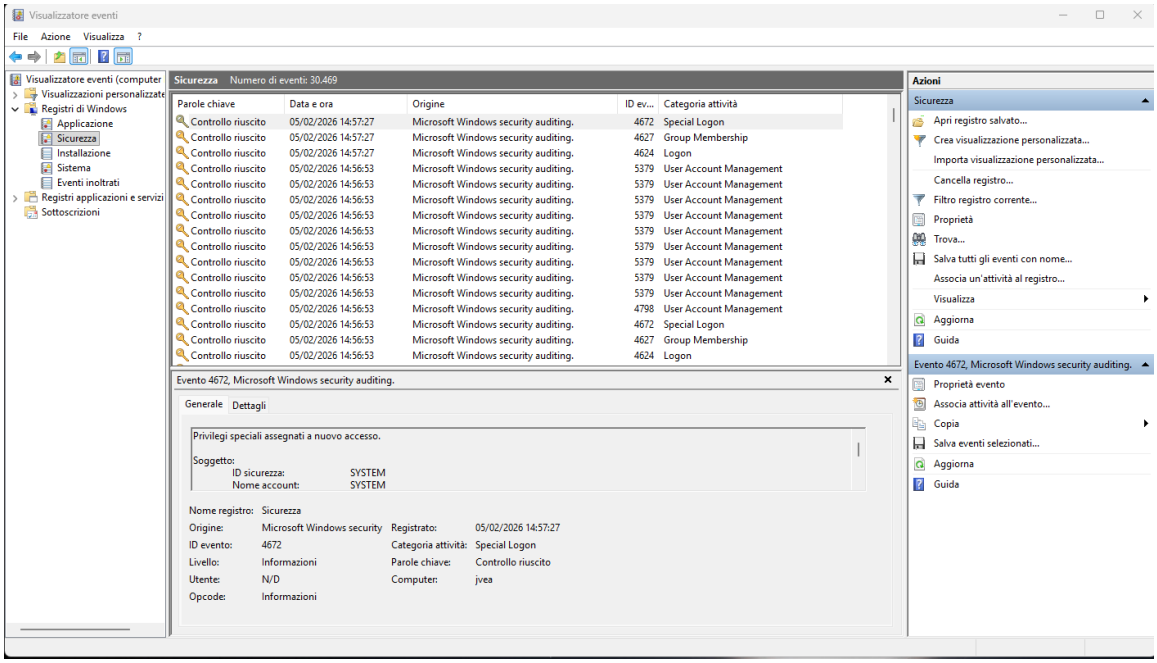
Listing 2: Dettagli Evento 4672

2.2.2 Evento ID 4624 - Logon Success

Contestualmente, è stato osservato l'evento **4624**, che registra l'avvenuto accesso di un account. Questo evento fornisce dettagli sull'utente specifico (nel nostro caso "JVEA") e il tipo di accesso effettuato.

2.2.3 Evento ID 4634 - Logoff

Per completare il ciclo di vita della sessione utente, è stato verificato l'evento di disconnessione (Logoff) identificato dall'ID **4634**. Questo evento viene generato quando una sessione di accesso viene terminata. La correlazione tra l'orario del Logon (4624) e del Logoff (4634) permette al SOC di calcolare la durata esatta della sessione e rilevare eventuali attività in orari non lavorativi.



Sicurezza Numero di eventi: 30.469

Parole chiave	Data e ora	Origine	ID ev...	Categoria attività
Controllo riuscito	05/02/2026 14:57:27	Microsoft Windows security auditing.	4672	Special Logon
Controllo riuscito	05/02/2026 14:57:27	Microsoft Windows security auditing.	4627	Group Membership
Controllo riuscito	05/02/2026 14:57:27	Microsoft Windows security auditing.	4624	Logon
Controllo riuscito	05/02/2026 14:56:53	Microsoft Windows security auditing.	5379	User Account Management
Controllo riuscito	05/02/2026 14:56:53	Microsoft Windows security auditing.	5379	User Account Management
Controllo riuscito	05/02/2026 14:56:53	Microsoft Windows security auditing.	5379	User Account Management
Controllo riuscito	05/02/2026 14:56:53	Microsoft Windows security auditing.	5379	User Account Management
Controllo riuscito	05/02/2026 14:56:53	Microsoft Windows security auditing.	5379	User Account Management
Controllo riuscito	05/02/2026 14:56:53	Microsoft Windows security auditing.	5379	User Account Management
Controllo riuscito	05/02/2026 14:56:53	Microsoft Windows security auditing.	5379	User Account Management
Controllo riuscito	05/02/2026 14:56:53	Microsoft Windows security auditing.	5379	User Account Management
Controllo riuscito	05/02/2026 14:56:53	Microsoft Windows security auditing.	5379	User Account Management
Controllo riuscito	05/02/2026 14:56:53	Microsoft Windows security auditing.	4798	User Account Management
Controllo riuscito	05/02/2026 14:56:53	Microsoft Windows security auditing.	4672	Special Logon
Controllo riuscito	05/02/2026 14:56:53	Microsoft Windows security auditing.	4627	Group Membership
Controllo riuscito	05/02/2026 14:56:53	Microsoft Windows security auditing.	4624	Logon

Evento 4672, Microsoft Windows security auditing.

Generale Dettagli

```
Privilegi speciali assegnati a nuovo accesso.

Soggetto:
        ID sicurezza:           SYSTEM
        Nome account:           SYSTEM
```

Nome registro:	Sicurezza		
Origine:	Microsoft Windows security	Registrato:	05/02/2026 14:57:27
ID evento:	4672	Categoria attività:	Special Logon
Livello:	Informazioni	Parole chiave:	Controllo riuscito
Utente:	N/D	Computer:	jvea
Opcode:	Informazioni		

Figura 2: Visualizzatore Eventi: Analisi dell'evento 4672 (Logon Speciale).

3 Conclusioni

L'attività di hardening è stata completata con successo.

1. La configurazione dei **Criteri di Controllo** locali è stata applicata correttamente, abilitando il tracciamento degli accessi riusciti e falliti.
2. Il sistema di logging sta registrando attivamente gli eventi nel registro **Security**, come dimostrato dalla presenza degli ID 4672, 4624, 4625.